A GENERALIZATION OF THE BOMBIERI-PILA DETERMINANT METHOD

OSCAR MARMON

ABSTRACT. The so called determinant method was developed by Bombieri and Pila in 1989 for counting integral points of bounded height on affine plane curves. In this paper we give a generalization of that method to varieties of higher dimension, yielding a proof of Heath-Brown's 'Theorem 14' by real-analytic considerations alone.

1. INTRODUCTION

In their paper [2], Bombieri and Pila used a determinant argument to get uniform estimates for the density of integral points on affine plane curves. Very roughly, the basic idea of the method can be described as follows: one constructs a collection of auxiliary polynomials, each vanishing at every integral point in a small square. This is done by forming a determinant of a suitable set of monomials evaluated at the integral points, which vanishes if the square is chosen small enough.

Heath-Brown [7] developed a non-archimedean version of the determinant method for counting rational points on projective hypersurfaces in any dimension. Whereas the original method of Bombieri and Pila can be said to use the archimedean absolute value to estimate the determinant, Heath-Brown instead groups together points that are p-adically close (for suitable primes p) and uses the p-adic absolute value to estimate the determinant. Salberger [10] has refined this method further, and it has turned out to be a very valuable tool for counting rational and integral points on algebraic varieties. One important feature of the method is that it produces uniform estimates for varieties of a given degree.

In this paper, we will revisit the determinant method in the real setting, and try to generalize it to higher dimensional varieties. This has been done to some extent, for example by Pila [9] and Pila and Wilkie [8], but the focus there is on non-algebraic sets, whereas we consider algebraic varieties. We shall recover the main theorem in [7] using only real-analytic considerations.

Thus, let $X \subset \mathbb{A}^n_{\mathbb{R}}$ be an irreducible closed subvariety. The main object of interest is, for a given positive real number B, the set of integral points of height at most B on X,

$$X(\mathbb{Z}, B) = \{\mathbf{x} = (x_1, \ldots, x_n) \in X \cap \mathbb{Z}^n; |x_i| \le B\}.$$

Its cardinality is denoted by $N(X, B)$. The following is our main result for affine varieties.

Theorem 1.1. *Let $X \subset \mathbb{A}_{\mathbb{R}}^n$ be an irreducible closed subvariety of dimension m and degree d. Let $I = I(X) \subset \mathbb{R}[x_1, \ldots, x_n]$ be the ideal of X. Then, for any $\varepsilon > 0$, there exists a polynomial $g \in \mathbb{Z}[x_1, \ldots, x_n] \setminus I$ of degree*

$$k \ll_{n,d,\varepsilon} B^{md^{-1/m}+\varepsilon},$$

all of whose irreducible factors have degree $O_{n,d,\varepsilon}(1)$, such that $g(\mathbf{x}) = 0$ for each $\mathbf{x} \in X(\mathbb{Z}, B)$.

Remark. By the dimension of X, we mean its dimension as an irreducible algebraic subset of $\mathbb{R}^n$ (see [1]). Thus it equals the Krull dimension of the ring $\mathbb{R}[x_1, \ldots, x_n]/I(X)$. It need not, however, equal the dimension of the variety $X_{\mathbb{C}} \subset \mathbb{A}_{\mathbb{C}}^n$ defined by the same equations, nor the dimension of the ring $\mathbb{R}[x_1, \ldots, x_n]/J$ for an arbitrary ideal J defining X.

We define the degree of X as the degree of its projective closure (see Section 3).

Theorem 1.1 allows us to use whatever estimates that may be available for varieties of dimension $m-1$ to bound $N(X, B)$. In case $m = 1$, the theorem produces a collection of curves of bounded degree harbouring all points of $X(\mathbb{Z}, B)$. Using Bézout's theorem, one concludes that $N(X, B) = O_{n,d,\varepsilon}(B^{1/d+\varepsilon})$, as in [2].

Theorem 1.1 is a corollary to our main result for projective varieties. The following notation will be used. We shall sometimes omit the ground field $\mathbb{R}$ and write $\mathbb{P}^n$ for $\mathbb{P}_{\mathbb{R}}^n$. The homothety class of $\mathbf{x} \in \mathbb{R}^{n+1}$ is denoted by $[\mathbf{x}]$. The set of rational points $\mathbb{P}^n(\mathbb{Q})$ consists of the points $x \in \mathbb{P}^n$ for which we can find a representative $\mathbf{x} \in \mathbb{Q}^{n+1}$ such that $[\mathbf{x}] = x$. If $X \subset \mathbb{P}^n$ is a locally closed subset, we define $X(\mathbb{Q}) = X \cap \mathbb{P}^n(\mathbb{Q})$.

We define the *height* of a rational point $x \in \mathbb{P}^n(\mathbb{Q})$ as follows. Choose a representative $\mathbf{x} \in \mathbb{Z}^{n+1}$ for x such that $\gcd(x_0, \ldots, x_n) = 1$ and put $H(x) = \max\{|x_0|, \ldots, |x_n|\}$. The density of rational points on X is measured by the counting function $N(X, \cdot)$ given by

$$N(X, B) = \#\{x \in X(\mathbb{Q}); H(x) \leq B\}.$$

for $B \in \mathbb{R}_{\geq 0}$. More generally, we wish to impose individual restrictions on the coordinates $x_0, \ldots, x_n$. Let $\mathbf{B} = (B_0, \ldots, B_n)$ be an $(n+1)$-tuple of positive real numbers. Then we define

$$S(X, \mathbf{B}) = \{\mathbf{x} \in \mathbb{Z}^{n+1}; [\mathbf{x}] \in X(\mathbb{Q}), |x_i| \leq B_i, i = 0, \ldots, n\}.$$

Following Broberg [3], we use graded monomial orderings to state our main result. These will be defined in Section 3. Given a monomial ordering $<$ and an irreducible projective variety $X \subseteq \mathbb{P}^n$, we associate

to the pair $(<, X)$ an $(n+1)$-tuple $(a_0, \ldots, a_n)$ of real numbers satisfying $0 \leq a_i \leq 1$ and $a_0 + \cdots + a_n = 1$ (see Proposition 3.2).

Theorem 1.2. *Let $X \subset \mathbb{P}_{\mathbb{R}}^n$ be an irreducible closed subvariety of dimension m and degree d, with ideal $I = I(X) \subset \mathbb{R}[x_0, \ldots, x_n]$. Let $\mathbf{B} = (B_0, \ldots, B_n)$ be an $(n+1)$-tuple of positive real numbers, and let $<$ be a graded monomial ordering on $\mathbb{R}[x_0, \ldots, x_n]$. Then, for any $\varepsilon > 0$, there is a homogeneous polynomial $G \in \mathbb{Z}[x_0, \ldots, x_n] \setminus I$ of degree*

$$k \ll_{n,d,\varepsilon} (B_0^{a_0} \cdots B_n^{a_n})^{(m+1)d^{-1/m}+\varepsilon},$$

all of whose irreducible factors have degree $O_{n,d,\varepsilon}(1)$, such that $G(\mathbf{x}) = 0$ for all $\mathbf{x} \in S(X, \mathbf{B})$.

We stress that this is not a new result (cf. Heath-Brown's original theorem [7, Thm 14] and Broberg's generalization [3, Thm 1]). Theorem 1.2 is proven in Section 5.

Acknowledgement. I am grateful to Jonathan Pila for introducing me to Gromov's lemma.

2. ESTIMATING A DETERMINANT

Let $U \subset \mathbb{R}^m$ be a compact subset. Consider a function $\psi : U \to \mathbb{R}$. For a multi-index $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_{\geq 0}^m$ we write

$$\partial^\alpha \psi = \frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_n}}{\partial x_n^{\alpha_n}} \psi.$$

We shall also use the following notation for multi-indices α:

$$|\alpha| = \alpha_1 + \cdots + \alpha_m,$$
$$\alpha! = \alpha_1! \cdots \alpha_m!.$$

If $\partial^\alpha \psi$ is defined and continuous for all α with $|\alpha| \leq k$ (in which case we write $\psi \in C^k(U)$), define the quantity

$$\|\psi\|_k = \max_{\mathbf{x} \in U} \max_{0 \leq |\alpha| \leq k} |\partial^\alpha \psi(\mathbf{x})|.$$

We shall investigate how $\|\cdot\|_k$ behaves under multiplication of functions.

Proposition 2.1. *Let $U \subset \mathbb{R}^m$ be a compact subset and suppose that $\phi_1, \ldots, \phi_\ell \in C^k(U)$. Then we have*

(1) $$\|\phi_1 \cdots \phi_\ell\|_k \leq \ell^k \|\phi_1\|_k \cdots \|\phi_\ell\|_k.$$

Proof. Suppose that α is a multi-index with $|\alpha| \leq k$. Using the product rule, we expand $\partial^\alpha(\phi_1 \cdots \phi_\ell)$ into a sum of $\ell^{|\alpha|}$ terms of the form

$$(\partial^{\alpha^1} \phi_1) \cdots (\partial^{\alpha^\ell} \phi_\ell),$$

where $\alpha^j \in \mathbb{Z}_{\geq 0}^m$ satisfy $\alpha^1 + \cdots + \alpha^\ell = \alpha$. Clearly we have

$$\sup_{\mathbf{x} \in U} |(\partial^{\alpha^1} \phi_1) \cdots (\partial^{\alpha^\ell} \phi_\ell)| \leq \|\phi_1\|_k \cdots \|\phi_\ell\|_k,$$

so the estimate (1) holds. $\qquad\square$

If $\mathbf{x} = (x_1, \ldots, x_m)$ is an m-tuple of indeterminates, and $\alpha \in \mathbb{Z}_{\geq 0}^m$, we write

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_m^{\alpha_m}.$$

Let us define the set $\Lambda_m(k)$ indexing monomials $\mathbf{x}^\alpha$ of degree k, that is,

$$\Lambda_m(k) = \{\mathbf{x}^\alpha \in \mathbb{Z}_{\geq 0}^m; |\alpha| = k\}.$$

Put $L_m(k) = \#\Lambda_m(k)$. In the same way, monomials of degree at most k are indexed by

$$\Delta_m(k) = \{\mathbf{x}^\alpha \in \mathbb{Z}_{\geq 0}^m; |\alpha| \leq k\} = \bigcup_{i=0}^{k} \Lambda_m(i).$$

Put $D_m(k) = \#\Delta_m(k)$. We have

$$L_m(k) = \binom{k + m - 1}{m - 1},$$

$$D_m(k) = \sum_{i=0}^{k} L_m(i) = \binom{k + m}{m}.$$

The following estimate is the starting point for the determinant method.

Lemma 2.1. *Let $\mu \in \mathbb{N}$. Let $U \subset \mathbb{R}^m$ be a compact convex set of diameter $r < 1$, and let $\psi_1, \ldots, \psi_\mu$ be real-valued C^ν functions on U. Given μ distinct points $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(\mu)}$ in U, define the $\mu \times \mu$-determinant*

$$\Delta = \det(\psi_i(\mathbf{x}^{(j)})).$$

Suppose that $\nu \in \mathbb{N}$ satisfies $D_m(\nu - 1) \leq \mu \leq D_m(\nu)$, and define

$$e = \sum_{i=0}^{\nu-1} i L_m(i) + \nu(\mu - D_m(\nu - 1)).$$

Then we have

(2)
$$|\Delta| \leq \mu! D_m(\nu)^\mu \prod_{i=1}^{\mu} \|\psi_i\|_\nu \cdot r^e.$$

Proof. We write each entry of Δ in the following form, using a Taylor expansion of order $\nu - 1$ around $\mathbf{x}^{(1)}$:

(3)
$$\psi_i(\mathbf{x}^{(j)}) = \sum_{|\alpha| \leq \nu - 1} \frac{\partial^\alpha \psi_i(\mathbf{x}^{(1)})}{\alpha!} (\mathbf{x}^{(j)} - \mathbf{x}^{(1)})^\alpha + R_\nu(\mathbf{x}^{(j)}).$$

Then there exists a point $\boldsymbol{\xi}_{ij}$ on the line segment joining $\mathbf{x}^{(1)}$ and $\mathbf{x}^{(j)}$ such that

$$R_\nu(\mathbf{x}^{(j)}) = \sum_{|\alpha| = \nu} \frac{\partial^\alpha \psi_i(\boldsymbol{\xi}_{ij})}{\alpha!} (\mathbf{x}^{(j)} - \mathbf{x}^{(1)})^\alpha.$$

The number of terms in each such sum is $D_m(\nu)$. Write each column in Δ as a sum of $D_m(\nu)$ column vectors according to (3), where each vector corresponds to a specific $\alpha \in \mathbb{Z}_{\geq 0}^m$. This gives an expansion of Δ as a sum of $D_m(\nu)^\mu$ determinants Δ_ℓ of the same dimension as Δ. However, any of these determinants possessing more than $L(i)$ columns corresponding to monomials of order i for any $i \leq \nu - 1$ has to vanish, since then these columns are linearly dependent. Consequently, the determinants Δ_ℓ satisfy

$$|\Delta_\ell| \leq \mu! \prod_{i=1}^{\mu} \|\psi_i\|_\nu \cdot r^e.$$

Summing over $1 \leq \ell \leq D_m(\nu)^\mu$ we get (2). $\qquad \square$

3. Monomial orderings and Hilbert functions

Let K be a field. We shall review the basics of Hilbert functions, following mainly the exposition in [5].

Definition. A *graded monomial ordering* on $K[x_0, \ldots, x_n]$ is a total ordering $<$ on $\mathbb{Z}_{\geq 0}^{n+1}$ (or equivalently on the set of monomials $\{\mathbf{x}^\alpha; \alpha \in \mathbb{Z}_{\geq 0}^{n+1}\}$) satisfying

    (1) $\forall \alpha \in \mathbb{Z}_{\geq 0}^{n+1}: \quad \alpha \geq \mathbf{0}$.
    (2) $\forall \alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^{n+1}: \quad \alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$.
    (3) $\forall \alpha, \beta \in \mathbb{Z}_{\geq 0}^{n+1}: \quad \alpha \leq \beta \Rightarrow |\alpha| \leq |\beta|$.

Given a graded monomial ordering $<$, we can define the *leading monomial* and *leading term* of a polynomial

$$f = \sum c_\alpha \mathbf{x}^\alpha \in K[x_0, \ldots, x_n]$$

as

$$\mathrm{LM}(f) = \mathbf{x}^\beta, \mathrm{LT}(f) = c_\beta \mathbf{x}^\beta, \text{ where } \beta = \max\{\alpha \in \mathbb{Z}_{\geq 0}^{n+1}; c_\alpha \neq 0\}.$$

For $s \in \mathbb{Z}_{\geq 0}$, let $K[x_0, \ldots, x_n]_s$ be the K-vector space of polynomials of degree s. A K-basis for $K[x_0, \ldots, x_n]_s$ is given by the set $L_n(s)$, defined in Section 2.

If $I \subseteq K[x_0, \ldots, x_n]$ is a homogeneous ideal, let $I_s = I \cap K[x_0, \ldots, x_n]_s$, a K-subspace of $K[x_0, \ldots, x_n]_s$. Define the *Hilbert function* of I,

$$\mathcal{H}_I : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0},$$

by

$$\mathcal{H}_I(s) = \dim_K \left(K[x_0, \ldots, x_n]_s / I_s \right).$$

For any ideal $I \subseteq K[x_0, \ldots, x_n]$, let $\mathrm{LT}(I)$ be the ideal generated by the leading terms of all the polynomials in I.

Proposition 3.1. *Let $I \subset K[x_0, \ldots, x_n]$ be a homogeneous ideal. Then $\mathcal{H}_I = \mathcal{H}_{\mathrm{LT}(I)}$. In other words, $\mathcal{H}_I(s)$ is the number of monomials of degree s that are not leading monomials of any $F \in I$.*

Proof. [5, Prop. 9, Ch. 9.3]   □

We shall also have use of the following functions, related to the Hilbert function. For each $i \in \{0, \ldots, n\}$, define

$$\sigma_{I,i}(s) = \sum_{\mathbf{x}^\alpha \in K[x_0, \ldots, x_n]_s \backslash \mathrm{LT}(I)} \alpha_i.$$

From Proposition 3.1 we see that

(4) $$\sigma_{I,0}(s) + \cdots + \sigma_{I,n}(s) = s\,\mathcal{H}_I(s).$$

Let $I \subset K[x_0, \ldots, x_n]$ be a homogeneous ideal, and suppose that I is generated by polynomials of degree at most δ. Then there are polynomials $P_I, Q_{I,0}, \ldots, Q_{I,n} \in \mathbb{Q}[t]$, and an integer s_0, depending only on n and δ, such that for every $s \geq s_0$ we have

$$\mathcal{H}_I(s) = P_I(s), \ \sigma_{I,0}(s) = Q_{I,0}(s), \ldots, \sigma_{I,n}(s) = Q_{I,n}(s).$$

Furthermore, the coefficients of $P_I, Q_{I,0}, \ldots, Q_{I,n}$ are also bounded in terms of n and δ. A proof of these statements can be found in [3]. P_I is called the *Hilbert polynomial* of I.

Let $X \subseteq \mathbb{P}_K^n$ be an irreducible variety, and let $I = I(X)$ be its ideal. We define the Hilbert function and Hilbert polynomial of X by $\mathcal{H}_X = \mathcal{H}_I$, $P_X = P_I$. The degree of P_X equals the dimension of X. Furthermore, if $m = \dim X$ and

$$P_X(t) = \sum_{i=0}^m a_i t^i,$$

then the *degree* of X is $\deg X = m! a_m$. By (4) we see that each of the $Q_{I,i}$ has degree at most $m+1$.

Remark 3.1. Given positive integers d and n, there is a finite set $\mathcal{F}_{n,d}$ of functions $\mathbb{Z}_{\geq 0} \to \mathbb{Z}$ such that $\mathcal{H}_X \in \mathcal{F}_{n,d}$ for all subvarieties $X \subset \mathbb{P}_K^n$ of degree d. (See [10, Lemma 1.4] and the references listed there.) In particular, all the coefficients of P_X can be bounded in terms of $\deg X$ and n.

From equation (4) and the following discussion, we draw the following conclusion.

Proposition 3.2. *Let $X \subseteq \mathbb{P}_K^n$ be an irreducible variety of degree d, and let I be its ideal. Then there are numbers $a_{I,i} \in [0,1]$ for $i \in \{0, \ldots, n\}$ such that*

(5) $$\frac{\sigma_{I,i}(s)}{s\,\mathcal{H}_I(s)} = a_{I,i} + O_{n,d}(1/s) \ as \ s \to \infty,$$

(6) $$a_{I,0} + \cdots + a_{I,n} = 1.$$

Remark 3.2 (Hilbert function and degree for affine varieties). For $s \in \mathbb{Z}_{\geq 0}$, let $K[x_1, \ldots, x_n]_{\leq s}$ be the vector space of polynomials of degree at most d. Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. Let $I_{\leq s} = I \cap K[x_1, \ldots, x_n]_{\leq s}$, a K-subspace of $K[x_1, \ldots, x_n]_{\leq s}$. Then we define the *affine Hilbert function* of I to be

$$\mathrm{H}_I(s) = \dim_K \left(K[x_1, \ldots, x_n]_{\leq s} / I_{\leq s} \right),$$

Consequently, if $X \subseteq \mathbb{A}_K^n$ is an irreducible variety, and I its ideal, we define $\mathrm{H}_X = \mathrm{H}_I$. However, if $I^h \subseteq K[x_0, \ldots, x_n]$ denotes the homogenization of I, and $\overline{X} \subseteq \mathbb{P}_K^n$ the projective closure of X (see [5, Ch. 8.4]), then by [5, Thm. 12, Ch. 9.3] we have $\mathrm{H}_X = \mathrm{H}_{I^h} = \mathcal{H}_I = \mathcal{H}_{\overline{X}}$. In particular, we can define the *degree* of X as

$$\deg X = \deg \overline{X}.$$

4. Gromov's algebraic lemma

In most applications of the determinant method, one uses the implicit function theorem to parametrize the points of a variety X. When applying a determinant estimate like Lemma 2.1, we have to bound the sizes of the partial derivatives of the implicit functions. In the original paper [2], this is done by excising the subset where the partial derivatives blow up, and covering it with smaller boxes, in which one carries out the method again, recursively. However, in a recent paper [8], Pila and Wilkie employ a more powerful method of parametrization, due to Gromov [6].

We extend the notions defined in Section 2 to vector-valued functions: a function $\phi : U \to \mathbb{R}^n$, where as before U is a compact subset of $\mathbb{R}^m$, belongs to the class C^k if all its coordinate functions do. In this case we define

$$\|\phi\|_k = \max_{\mathbf{x} \in U} \max_{0 \leq |\alpha| \leq k} |\partial^\alpha \phi(\mathbf{x})|,$$

where $|(x_1, \ldots, x_n)| = \max_i |x_i|$. Now we can formulate Gromov's lemma. The proof in [6] is rather brief, but Burguet [4] has given a more detailed proof. Another proof can be extracted from that of Pila and Wilkie [8] in the more general setting of definable sets.

Lemma 4.1. *Let $V \subset \mathbb{A}_{\mathbb{R}}^n$ be an algebraic variety of dimension $m < n$ and degree d, and let $Y = V \cap [-1, 1]^n$. For each $r \in \mathbb{Z}_+$, there exists an integer N_0, depending only on n, r and d, and C^r-functions $\phi_i : [-1, 1]^m \to Y$ for $i = 1, 2, \ldots, N_0$, such that*

$$\bigcup_{i=1}^{N_0} \phi_i([-1, 1]^m) = Y \text{ and } \|\phi_i\|_r \leq 1.$$

Our formulation differs from Gromov's on two points. Firstly, we use the $[-1, 1]^m$ and $[-1, 1]^n$ instead of $[0, 1]^m$ and $[0, 1]^n$. It is completely obvious that these two cases give equivalent statements. Secondly, we

claim that N_0 is bounded in terms of the degree of Y, whereas Gromov uses the sum of the degrees of a collection of polynomials defining Y. To see that our statement follows from Gromov's, we make the following remark.

Remark 4.1. By Remark 3.1, given $d = \deg Y$, we have only finitely many choices for the Hilbert function $\mathcal{H}_Y$, and thus for the Hilbert polynomial P_Y. By considering the Hilbert scheme of closed subschemes of $\mathbb{P}_K^n$ having Hilbert polynomial $P = P_Y$, one gets homogeneous polynomials defining $\overline{Y}$, whose number and degree are bounded in terms of n and d (see [10, Lemma 1.3]). Dehomogenizing, we get defining polynomials for Y.

5. Rational points on projective varieties

In this section we shall prove Theorem 1.2. To begin with, we have

$$S(X, \mathbf{B}) = \bigcup_{i=0}^{n} S_i(X, \mathbf{B}),$$

where $S_i(X, \mathbf{B})$ is the set of $\mathbf{x} \in S(X, \mathbf{B})$ such that $|x_j/B_j| \leq |x_i/B_i|$ for all $j \in \{0, \ldots, n\}$. Thus, let $i \in \{0, \ldots, n\}$. We shall find a form vanishing at every point of $S_i(X, \mathbf{B})$. By permuting the variables, we can assume that $i = 0$.

Let $\tau : \mathbb{R}^n \to \mathbb{R}^n$ be given by

$$\tau(x_0, \ldots, x_n) = \left(\frac{1}{B_0} x_0, \ldots, \frac{1}{B_n} x_n \right).$$

τ induces an automorphism $\bar{\tau} : \mathbb{P}_{\mathbb{R}}^n \to \mathbb{P}_{\mathbb{R}}^n$. Let $Z \subset \mathbb{P}_{\mathbb{R}}^n$ be the image of X under $\bar{\tau}$. Furthermore, let

$$T_0(X, \mathbf{B}) = \tau(S_0(X, \mathbf{B})) \subseteq [-1, 1]^{n+1} \cap \mathbb{R}^{n+1}.$$

Let $\iota_0 : \mathbb{A}_{\mathbb{R}}^n \to \mathbb{P}_{\mathbb{R}}^n$ be the open immersion given by

$$(z_1, \ldots, z_n) \mapsto [(1, z_1, \ldots, z_n)],$$

and let $Z_0 = \iota_0^{-1}(Z)$. By Remark 3.2 we have $\deg Z_0 = \deg Z = \deg X$. Note also that $\left| \iota_0^{-1}([\mathbf{y}]) \right| \leq 1$ if $\mathbf{y} \in T_0(X, \mathbf{B})$.

For any $\delta \in \mathbb{Z}_{\geq 0}$, define

$$M(\delta) = \{ \mathbf{e} \in \mathbb{Z}_{\geq 0}^{n+1}; |\mathbf{e}| = \delta, \mathbf{x}^{\mathbf{e}} \notin \mathrm{LT}(I) \}.$$

We say that a polynomial G is *defined in* $M(\delta)$ if $\mathbf{e} \in M(\delta)$ for all monomials $\mathbf{x}^{\mathbf{e}}$ occurring in G. If this is the case, then $G \notin I$.

Write $\sigma_i = \sigma_{I,i}(\delta)$, that is

(7)
$$\sigma_i = \sum_{\mathbf{e} \in M(\delta)} e_i.$$

Put $\mu = |M(\delta)|$, which by Proposition 3.1 equals $\mathcal{H}_I(\delta)$, and choose the integer ν so that

$$(8) \qquad\qquad D_m(\nu - 1) \leq \mu \leq D_m(\nu).$$

Define

$$(9) \qquad\qquad f = \sum_{i=0}^{\nu-1} i L_m(i) + \nu(\mu - D_m(\nu - 1)).$$

By Gromov's lemma, there is a collection of C^ν functions $\phi_1, \ldots, \phi_N$: $[-1,1]^m \to [-1,1]^n$, such that $\|\phi_i\|_\nu \leq 1$, and whose images cover $Z_0 \cap [-1,1]^n$. The number of functions needed, N, depends only upon n, d and δ. Let $\phi \in \{\phi_1, \ldots, \phi_N\}$, and define

$$S_{0,\phi}(X, \mathbf{B}) = \{\mathbf{x} \in S_0(X, \mathbf{B}); \bar{\tau}([\mathbf{x}]) \in \iota_0(\mathrm{im}\,\phi)\}.$$

Then we want to find a collection $\mathcal{G} = \{G_1, \ldots, G_k\}$ of homogeneous polynomials defined in $M(\delta)$ such that for each $\mathbf{x} \in S_{0,\phi}(X, \mathbf{B})$, there is a polynomial $G \in \mathcal{G}$ such that $G(\mathbf{x}) = 0$. We shall prove that this is possible with k satisfying

$$(10) \qquad\qquad k \ll_{n,d,\delta} B_0^{m\sigma_0/f} \cdots B_n^{m\sigma_n/f},$$

where σ_i and f are as defined in (7) and (9). Multiplying these forms together, we get a form of degree δk, vanishing at each point of $S_{0,\phi}(X, \mathbf{B})$ but not belonging to I, and whose irreducible factors all have degree at most δ. Having proven this, we shall then choose δ as to give the desired estimate.

To prove the estimate (10), we consider a covering of $[-1,1]^m$ by cubes Σ of sidelength ρ, where the value of ρ is to be chosen appropriately later on in the proof. For a certain fixed cube Σ, let $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(q)}$ be an enumeration of the (finitely many) points in $S_{0,\phi}(X, \mathbf{B})$ such that $\bar{\tau}([\mathbf{x}]) \in \iota_0(\phi(\Sigma))$. We shall then find a polynomial G, with integral coefficients and defined in $M(\delta)$, such that

$$(11) \qquad\qquad G(\mathbf{x}^{(1)}) = \cdots = G(\mathbf{x}^{(q)}) = 0.$$

We shall achieve this by bounding the rank of the matrix

$$\mathcal{A} = \left((\mathbf{x}^{(j)})^{\mathbf{e}}\right)_{\substack{\mathbf{e} \in M(\delta) \\ j=1,\ldots,q}},$$

with rows corresponding to exponent $(n+1)$-tuples $\mathbf{e}$, ordered according to the chosen graded monomial order $<$, and columns corresponding to the different points $\mathbf{x}^{(j)}$. We will prove that $\mathcal{A}$ has rank at most $\mu - 1$, thus producing a polynomial satisfying (11), as in [2, Lemma 1].

If $q \leq \mu - 1$, then of course $\mathrm{rank}\,\mathcal{A} \leq \mu - 1$. Assume therefore that $q \geq \mu$, and pick μ points among the $\mathbf{x}^{(j)}$. Renumber the points as $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\mu)}$. We shall now examine the determinant

$$\mathcal{D} = \det\left((\mathbf{x}^{(j)})^{\mathbf{e}}\right)_{\substack{\mathbf{e} \in M(\delta) \\ j=1,\ldots,\mu}}.$$

Let $\mathbf{y}^{(j)} = \tau(\mathbf{x}^{(j)}) \in [-1,1]^{n+1}$. Then we have

$$\mathcal{D} = B_0^{\sigma_0} \cdots B_n^{\sigma_n} \mathcal{D}', \text{ where } \mathcal{D}' = \det \left((\mathbf{y}^{(j)})^{\mathbf{e}} \right)_{\substack{\mathbf{e} \in M(\delta) \\ j=1,\ldots,\mu}}.$$

Writing $\mathbf{z}^{(j)} = (y_1^{(j)}/y_0^{(j)}, \ldots, y_n^{(j)}/y_0^{(j)})$, we have $\mathbf{z}^{(j)} \in \phi(\Sigma)$ by assumption. Furthermore, we have

$$\mathcal{D}' = \left(y_0^{(1)} \cdots y_0^{(\mu)} \right)^{\delta} \Delta, \text{ where } \Delta = \det \left((1, \mathbf{z}^{(j)})^{\mathbf{e}} \right)_{\substack{\mathbf{e} \in M(\delta) \\ j=1,\ldots,\mu}},$$

so $|\mathcal{D}'| \leq |\Delta|$. To estimate Δ, we can now use Lemma 2.1. Enumerating the elements $\mathbf{e}(1), \ldots, \mathbf{e}(\mu)$ of $M(\delta)$ as specified by $<$, we let the functions $\psi_i : \Sigma \to \mathbb{R}$ in the hypothesis of the lemma be given by

$$\psi_i(\mathbf{u}) = (1, \phi(\mathbf{u}))^{\mathbf{e}(i)}.$$

Using Proposition 2.1, together with the fact that $\|\phi\|_{\nu} \leq 1$, we see that $\|\psi_i\| \ll_{n,d,\delta} 1$. Thus we get $|\Delta| \ll_{n,d,\delta} \rho^f$, so that

$$|\mathcal{D}| \ll_{n,d,\delta} B_0^{\sigma_0} \cdots B_n^{\sigma_n} \rho^f.$$

Now we make use of the crucial fact that the entries in $\mathcal{D}$ are all integers, from which follows that either $\mathcal{D} = 0$ or $|\mathcal{D}| \geq 1$. We see that if we choose

$$B_0^{-\sigma_0/f} \cdots B_n^{-\sigma_n/f} \ll_{n,d,\delta} \rho \ll_{n,d,\delta} B_0^{-\sigma_0/f} \cdots B_n^{-\sigma_n/f},$$

we will get $|\mathcal{D}| < 1$, and consequently $\mathcal{D} = 0$. Thus, for each small cube Σ we produce a polynomial G, defined in $M(\delta)$, with the desired property. To cover $[-1,1]^m$ we do not need more than

$$O_{n,d,\delta}(B_0^{m\sigma_0/f} \cdots B_n^{m\sigma_n/f})$$

of the cubes Σ, so the estimate (10) follows.

We have now proven that there exists a form $G \notin I$ of degree k vanishing at every point in $S(X, \mathbf{B})$, where k satisfies (10). Furthermore, the irreducible factors of G have degree at most δ. It remains to choose the value of the parameter δ. By Proposition 3.2, we have

$$\sigma_i = a_i \delta \, \mathcal{H}(\delta) + O_{n,d}(\delta^m) = \frac{a_i d}{m!} \delta^{m+1} + O_{n,d}(\delta^m).$$

as $\delta \to \infty$. Furthermore, our choice (8) implies that

$$\nu = d^{1/m} \delta + O_{n,d}(1),$$

so we have

$$f = \sum_{i=0}^{\nu} i L_m(i) + O_m(\nu^m) = \frac{\nu^{m+1}}{(m+1)(m-1)!} + O_m(\nu^m)$$

$$= \frac{d^{(m+1)/m}}{(m+1)(m-1)!} \delta^{m+1} + O_{n,d}(\delta^m).$$

This yields
$$\frac{m\sigma_i}{f} = \frac{(m+1)a_i}{d^{1/m}} + O_{n,d}(\delta^{-1}).$$
In particular, we can choose δ depending only on n, d and ε, such that
$$\frac{m\sigma_i}{f} \leq \frac{(m+1)a_i}{d^{1/m}} + \varepsilon.$$
This concludes the proof of Theorem 1.2.

6. INTEGRAL POINTS ON AFFINE VARIETIES

In this section we prove Theorem 1.1. Let $X \subset \mathbb{A}_{\mathbb{R}}^n$ be an irreducible closed subvariety of dimension m and degree d, and let $I = I(X) \subset \mathbb{R}[x_1, \ldots, x_n]$. Let $\overline{X} \subset \mathbb{P}_{\mathbb{R}}^n$ be the projective closure of X [5, §8.4]. Then the homogeneous ideal of $\overline{X}$ is the homogenization I^h of I. Furthermore, let $\mathbf{B} = (1, B, \ldots, B) \in \mathbb{R}^{n+1}$. If $(x_1, \ldots, x_n) \in X(\mathbb{Z}, B)$, then $(1, x_1, \ldots, x_n) \in S(\overline{X}, \mathbf{B})$.

By Theorem 1.2, given a graded monomial ordering $<$, there exists a homogeneous polynomial $G \in \mathbb{Z}[x_0, \ldots, x_n] \setminus I^h$ of degree
$$k \ll_{n,d,\varepsilon} B^{(a_1+\cdots+a_n)(m+1)d^{-1/m}}$$
such that $G(\mathbf{x}) = 0$ for all $\mathbf{x} \in S(\overline{X}, \mathbf{B})$.

Put
$$g(x_1, \ldots, x_n) = G(1, x_1, \ldots, x_n).$$
Then $g \notin I$ since $G \notin I^h$, and we have $g(\mathbf{x}) = 0$ for every $\mathbf{x} \in X(\mathbb{Z}, B)$. To complete the proof of Theorem 1.1, we only have to prove that $<$ can be chosen in such a way that

(12)
$$a_1 + \cdots + a_n \leq \frac{m}{m+1}.$$

We shall follow the proof of [10, Lemma 1.12], defining the graded monomial ordering by letting $\mathbf{x}^\alpha < \mathbf{x}^\beta$ if and only if $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and the left-most entry of $\alpha - \beta$ is positive. We need to examine, for $s \in \mathbb{Z}_{\geq 0}$, the quantity
$$\sigma_1(s) + \ldots + \sigma_n(s) = \sum_{\mathbf{x}^\alpha \in L_{n+1}(s) \setminus \mathrm{LT}(I^h)} (\alpha_1 + \ldots + \alpha_n).$$
Suppose that
$$L_{n+1}(s) \setminus \mathrm{LT}(I^h) = \{M_1, \ldots, M_h\},$$
where $h = \mathcal{H}_{I^h}(s)$. Put $m_i(x_1, \ldots, x_n) = M_i(1, x_1, \ldots, x_n)$ for $i \in \{1, \ldots, h\}$. Then we have

(13)
$$\sigma_1(s) + \ldots + \sigma_n(s) = \deg m_1 + \ldots \deg m_h.$$

Now, let $J \subset \mathbb{R}[x_0, \ldots, x_n]$ be the homogeneous ideal generated by I^h and x_0. We claim that

(14)
$$m_i \notin \mathrm{LT}(J), \text{ for } i = 1, \ldots, h.$$

Indeed, if m_i were the leading monomial of $F = x_0 G + H$, where $H \in I^h$, then $M_i = x_0^{s - \deg m_i} m_i$ would be the leading monomial of $x_0^{s - \deg m_i} H \in I^h$.

Since the m_i are distinct, (13) and (14) imply that

$$\sigma_1(s) + \ldots + \sigma_n(s) \leq \sum_{t=1}^{s} t \, \mathcal{H}_J(t).$$

For the variety $X_0 = \overline{X} \cap H_0$ defined by J we have

$$\deg X_0 \leq \deg X, \quad \dim X_0 \leq m - 1,$$

so

$$\mathcal{H}_J(t) \leq \frac{d}{(m-1)!} t^{m-1} + O_{n,d}(t^{m-2}),$$

whence

$$\sum_{t=1}^{s} t \, \mathcal{H}_J(t) \leq \frac{d}{(m+1)(m-1)!} s^{m+1} + O_{n,d}(s^m).$$

Thus we get

$$\frac{\sigma_1(s) + \ldots + \sigma_n(s)}{s \, \mathcal{H}_{I^h}(s)} \leq \frac{m}{m+1} + O_{n,d}(s^{-1}).$$

By Proposition 3.2 we conclude that (12) holds. This completes the proof of Theorem 1.1.

References

[1] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle*, volume 12 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1987.

[2] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.

[3] Niklas Broberg. A note on a paper by R. Heath-Brown: "The density of rational points on curves and surfaces" [Ann. of Math. (2) **155** (2002), no. 2, 553–595; mr1906595]. *J. Reine Angew. Math.*, 571:159–178, 2004.

[4] David Burguet. A proof of Gromov's algebraic lemma. Preprint, arXiv:math/0509277v2.

[5] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra.

[6] M. Gromov. Entropy, homology and semialgebraic geometry. *Astérisque*, (145-146):5, 225–240, 1987. Séminaire Bourbaki, Vol. 1985/86.

[7] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. of Math. (2)*, 155(2):553–595, 2002.

[8] J. Pila and A. J. Wilkie. The rational points of a definable set. *Duke Math. J.*, 133(3):591–616, 2006.

[9] Jonathan Pila. Integer points on the dilation of a subanalytic surface. *Q. J. Math.*, 55(2):207–223, 2004.

[10] Per Salberger. On the density of rational and integral points on algebraic varieties. *J. Reine Angew. Math.*, 606:123–147, 2007.